A – 12

Suatu Algoritma Kriptografi Simetris Berdasarkan Jaringan Substitusi-Permutasi Dan Fungsi Affine Atas Ring Komutatif Z_n

Muhamad Zaki Riyanto
Pendidikan Matematika, JPMIPA, FKIP
Universitas Ahmad Dahlan, Yogyakarta
E-mail: zakimath@gmail.com
http://zaki.math.web.id

Abstrak

Salah satu solusi dalam pengamanan pengiriman pesan rahasia adalah menggunakan kriptografi, yaitu menggunakan proses enkripsi-dekripsi. Pada proses enkripsi, pesan rahasia (plainteks) dirubah menjadi pesan acak yang sulit dimengerti (cipherteks). Sedangkan proses dekripsi berfungsi untuk mengembalikan cipherteks ke plainteks. Kedua proses ini menggunakan suatu mekanisme dan kunci tertentu.
Salah satu mekanisme dalam kriptogafi adalah algoritma kriptografi simetris, yaitu proses enkripsi dan dekripsi menggunakan kunci yang sama. Dalam perkembangannya, saat ini yang telah dikenal luas adalah algoritma AES (*Advanced Encryption Standard*). Algoritma tersebut didasarkan pada metode jaringan substitusi-permutasi atau lebih dikenal dengan *Substitution-Permutation Network* (SPN).
Stinson (2006) telah memberikan sebuah contoh sederhana dari SPN menggunakan bilangan biner dan heksadesimal. Dalam makalah ini diberikan sebuah pengembangan dari SPN, yaitu menggunakan ring komutatif Z_n. Pada makalah ini contoh yang digunakan adalah ring komutatif Z_{26} yang berkorespondensi dengan himpunan semua huruf alfabet dari A sampai Z. Proses subtitusi menggunakan fungsi affine berupa matriks persegi invertibel atas Z_{26} dan vektor konstan, sedangkan proses permutasi menggunakan suatu permutasi pada grup permutasi. Proses substitusi dan permutasi ini dilakukan dalam beberapa perulangan. Hal ini dilakukan dengan harapan agar plainteks yang dihasilkan menjadi terlihat acak, sehingga akan mempersulit pihak musuh untuk memecahkan pesan rahasia.
Kata kunci: Enkripsi, dekripsi, matriks invertibel, ring komutatif, *Substitution-Permutation Network*

1. Pendahuluan

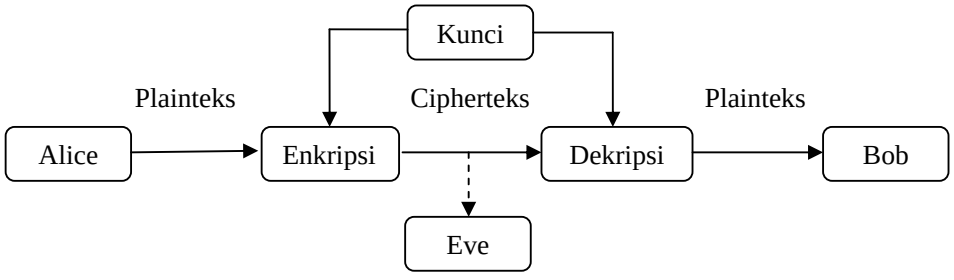
Sebagai makhluk sosial, manusia sering melakukan komunikasi dengan orang lain. Mereka saling bertukar informasi, baik berupa informasi yang bersifat umum maupun informasi yang bersifat rahasia. Informasi yang bersifat rahasia tersebut hanya boleh diketahui oleh orang-orang tertentu saja. Bila informasi rahasia tersebut jatuh ke tangan orang yang tidak berhak untuk mengetahui isi informasi tersebut, maka akan dapat menimbulkan kerugian dan hal-hal yang tidak diinginkan.

Perkembangan teknologi informasi dewasa ini telah berpengaruh pada hampir semua aspek kehidupan manusia, tak terkecuali dalam hal berkomunikasi. Dengan adanya internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan murah. Namun di sisi lain, ternyata internet tidak terlalu aman karena merupakan jalur komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap

penyadapan. Oleh karena itu, keamanan informasi menjadi faktor utama yang harus dipenuhi.

Salah satu solusi yang dapat digunakan untuk menyelesaikan masalah tersebut adalah menggunakan kriptografi. Kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes dkk, 1996). Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain. Enkripsi adalah suatu proses penyandian yang melakukan perubahan suatu pesan, dari yang dapat dimengerti, disebut dengan plainteks, menjadi suatu kode yang sulit dimengerti, disebut dengan cipherteks. Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut dekripsi. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu.

Algoritma kriptografi (sistem kriptografi) atau sering disebut dengan *cipher* merupakan suatu sistem atau kumpulan aturan-aturan (algoritma) yang digunakan untuk melakukan enkripsi dan dekripsi. Algoritma kriptografi simetris adalah algoritma kriptografi yang menggunakan kunci enkripsi dan dekripsi yang sama. Sistem ini mengharuskan dua pihak yang berkomunikasi menyepakati suatu kunci rahasia yang sama sebelum keduanya saling berkomunikasi. Keamanan dari sistem ini tergantung pada kunci, membocorkan kunci berarti bahwa orang lain yang berhasil mendapatkan kunci dapat mendekripsi cipherteks. Algoritma kriptografi ini sering disebut juga dengan algoritma kriptografi kunci rahasia, seperti dijelaskan pada gambar berikut ini.



Gambar 1. Algoritma Kriptografi Simetris

Pada Gambar 1 di atas, ada dua pihak yaitu Alice dan Bob yang berkomunikasi secara rahasia menggunakan algoritma kriptografi simetris. Komunikasi dilakukan melalui jalur komunikasi yang tidak dapat dijamin keamanannya. Untuk dapat melakukan komunikasi secara rahasia, Alice dan Bob harus menyetujui suatu kunci rahasia yang sama. Akan tetapi, ada pihak ketiga yaitu Eve yang berada di antara kedua pihak yang berusaha untuk rmendapatkan informasi rahasia yang dikirimkan. Contoh algoritma kriptografi simetris adalah DES, Blowfish, dan AES (*Advanced Encryption Standard*). Saat ini AES merupakan algoritma kriptografi simetris yang digunakan secara luas di internet. Dalam melakukan proses enkripsi-dekripsi, AES menggunakan metode Jaringan Substitusi-Permutasi.

Stinson (2006) telah memberikan penjelasan dan contoh kasus dari Jaringan Substitusi-Permutasi. Dalam makalah ini dijelaskan mengenai algoritma kriptografi simetris yang didasarkan pada Jaringan Substitusi-Permutasi yang didefinisikan atas lapangan hingga $Z_2 = \{0,1\}$ atau bilangan biner. Selanjutnya, diberikan pengembangan dari algoritma tersebut menggunakan sebarang ring komutatif $Z_n = \{0,1,2,...,n-1\}$. Dalam makalah ini diberikan contoh menggunakan ring komutatif $Z_{26} = \{0,1,2,...,25\}$ yang berkorespondensi dengan himpunan semua huruf alfabet A sampai dengan Z. Salah satu metode yang digunakan dalam pengembangan tersebut adalah menggunakan fungsi affine dengan perkalian matriks invertibel atas ring Z_n.

2. Jaringan Substitusi-Permutasi

Jaringan Substitusi-Permutasi atau dikenal dengan *Substitution-Permutation Network* (SPN) merupakan salah satu metode dalam melakukan proses enkripsi dan dekripsi. Metode ini menggunakan iterasi atau perulangan dari proses substitusi, permutasi dan penjumlahan kunci. Stinson (2006) memberikan suatu contoh algoritma kriptografi simetris yang berbasis pada Jaringan Substitusi-Permutasi sebagai berikut.

Sistem dasar SPN ini dibentuk dari dua permutasi, yaitu π_S dan π_P, dimana $\pi_S : \{0,1\}^k \to \{0,1\}^k$, dan $\pi_P : \{1,...,km\} \to \{1,...,km\}$. Permutasi π_S disebut dengan S-box, digunakan untuk proses substitusi suatu *k* bit dengan suatu *k* bit yang lain. Sedangkan permutasi π_P digunakan untuk proses permutasi suatu *km* bit. Didefinisikan

P adalah himpunan semua plainteks, C adalah himpunan semua cipherteks dan K adalah himpunan semua kunci. Diberikan *k*, *m* dan *Nr* adalah suatu bilangan bulat positif. Diberikan suatu permutasi $\pi_S : \{0,1\}^k \to \{0,1\}^k$ dan permutasi $\pi_P : \{1,...,km\} \to \{1,...,km\}$. Didefinisikan P = C = $\{0,1\}^{km}$ dan K Í $\left(\{0,1\}^{km}\right)^{Nr+1}$ memuat semua kunci yang mungkin yang dapat diturunkan dari kunci awal menggunakan suatu algoritma penjadwalan kunci (*key scheduling*). Untuk suatu penjadwalan kunci yang terdiri dari *round key – round key* yaitu $(K^1,...,K^{Nr+1})$, proses enkripsinya diberikan pada algoritma berikut ini.

Algoritma: SPN $(x, p_S, p_P, (K^1,...,K^{Nr+1}))$

$w^0 \neg x$

for $r \neg 1$ **to** $Nr - 1$

do { $u^r \neg w^{r-1} \text{Å} K^r$

for $i \neg 1$ **to** m

do { $v^r_{<i>} \neg p_S(u^r_{<i>})$ **}**

$w^r \neg (v^r_{p_P(1)},...,v^r_{p_P(km)})$ **}**

$u^{Nr} \neg w^{Nr-1} \text{Å} K^{Nr}$

for $i \neg 1$ **to** m

do { $v^{Nr}_{<i>} \neg p_S(u^{Nr}_{<i>})$ **}**

$y \neg v^{Nr} \text{Å} K^{Nr+1}$

output(*y*)

Gambar 2. Algoritma SPN (Stinson, 2006)

Diberikan suatu plainteks berupa string biner dengan panjang *km* bit, misalkan $x = (x_1, x_2,..., x_{km})$. Selanjutnya, pada *x* dapat dibentuk *m* substring, masing-masing *k* bit, dan dinotasikan dengan $x_{<1>}, x_{<2>},..., x_{<m>}$. Sehingga $x = x_{<1>} \| x_{<2>} \| ... \| x_{<m>}$ dan untuk $1 £ i £ m$ diperoleh $x_{<i>} = (x_{(i-1)k+1},..., x_{ik})$. SPN mempunyai *Nr* putaran (*round*). Setiap putaran (kecuali pada putaran terakhir) dilakukan *m* substitusi menggunakan π_S

dan langsung diikuti dengan permutasi menggunakan π_P. Pada algoritma SPN di atas, u^r dimasukkan ke dalam S-box (pada putaran ke-*r*) dan ouputnya adalah v^r. Untuk w^r diperoleh dari v^r dengan menggunakan permutasi π_P, dan u^{r+1} dikonstruksi dari w^r dengan meng-*xor* dengan ***round key*** K^{r+1}. Proses ini disebut dengan ***round key mixing***. Perhatikan bahwa pada putaran terakhir, permutasi π_P tidak digunakan.

Berikut ini diberikan sebuah contoh enkripsi menggunakan SPN. Pada contoh ini digunakan penulisan heksadesimal (Hex) seperti diberikan pada tabel di bawah ini.

Tabel 1. Tabel Heksadesimal-Biner

Biner	Hex
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7

Biner	Hex
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Diberikan $k = m = Nr = 4$. Didefinisikan S-box dengan π_S sebagai berikut.

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Selanjutnya, didefinisikan π_P sebagai berikut.

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_P(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Misalkan diberikan kunci K = `0011 1010 1001 0100 1101 0110 0011 1111`. Selanjutnya, dapat didefinisikan algoritma penjadwalan kunci dengan *round key* :

K^1 = `0011 1010 1001 0100` K^4 = `0100 1101 0110 0011`

K^2 = `1010 1001 0100 1101` K^5 = `1101 0110 0011 1111`.

K^3 = 1001 0100 1101 0110

Misal diberikan plainteks x = 0010 0110 1011 0111. Proses enkripsi akan berjalan seperti berikut ini:

w^0 = 0010 0110 1011 0111

K^1 = 0011 1010 1001 0100

u^1 = 0001 1100 0010 0011

v^1 = 0100 0101 1101 0001

w^1 = 0010 1110 0000 0111

K^2 = 1010 1001 0100 1101

u^2 = 1000 0111 0100 1010

v^2 = 0011 1000 0010 0110

w^2 = 0100 0001 1011 1000

K^3 = 1001 0100 1101 0110

u^3 = 1101 0101 0110 1110

v^3 = 1001 1111 1011 0000

w^3 = 1110 0100 0110 1110

K^4 = 0100 1101 0110 0011

u^4 = 1010 1001 0000 1101

v^4 = 0110 1010 1110 1001

K^5 = 1101 0110 0011 1111

y = 1011 1100 1101 0110

Diperoleh cipherteks y = 1011 1100 1101 0110. Proses dekripsi pada SPN dapat dipelajari dengan membalik proses enkripsi, sedangkan permutasi yang digunakan adalah invers dari permutasi $\pi_S(z)$ dan $\pi_P(z)$. Round key yang digunakan mulai dari K^5, K^4, K^3, K^2, dan K^1.

3. Jaringan Substitusi-Permutasi atas Ring Komutatif Z_n

Algoritma kriptografi simetris yang menggunakan metode Jaringan Substitusi-Permutasi di atas dapat dikembangkan menggunakan ring komutatif $Z_n = \{0,1,2,...,n-1\}$. Pada proses substitusi menggunakan fungsi affine berupa

perkalian matriks invertibel atas Z_n dan diikuti dengan penjumlahan vektor konstan. Berikut ini diberikan beberapa sifat dari Z_n.

Teorema 1. *Suatu elemen* $a \in Z_n$ *mempunyai invers* (*terhadap perkalian*) *dalam* Z_n *jika dan hanya jika* $\text{fpb}(a,n)=1$, *yaitu a relatif prima dengan n.*

Teorema 1 di atas mengakibatkan bahwa jika *p* adalah bilangan prima, maka Z_p merupakan lapangan. Sebagai contoh, Z_2 merupakan lapangan. Fungsi affine dalam proses substitusi menggunakan perkalian matriks invertibel atas Z_n. Berikut ini diberikan sifat mengenai matriks invertibel atas Z_n.

Teorema 2. *Diberikan matriks* $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *dengan* $a,b,c,d \in Z_n$, *maka A mempunyai invers* (*terhadap perkalian*) *dalam* Z_n *jika dan hanya jika* $\text{fpb}(ad-bc,n)=1$.

Dinotasikan $GL_2(Z_n)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in Z_n,\ \text{fpb}(ad-bc,n)=1\right\}$ adalah himpunan semua matriks invertibel atas Z_n. Selanjutnya, diberikan himpunan semua vektor $Z_n^2=\left\{\begin{pmatrix} s \\ t \end{pmatrix} \middle| s,t \in Z_n\right\}$. Diberikan grup permutasi

$$S_m=\left\{\begin{pmatrix} 1 & 2 & \cdots & m \\ p(1) & p(2) & \cdots & p(m) \end{pmatrix} \middle| p:\{1,2,...,m\}\to\{1,2,...,m\} \text{ bijektif}\right\}.$$

Algoritma enkripsi dan dekripsi serta penjadwalan kunci diberikan sebagai berikut. Diberikan plainteks $X = x_1x_2\ x_3x_4\ x_5x_6\ x_7x_8\ x_9x_{10}$, dengan $x_i \in Z_n$, $i=1,2,...,10$.

Sebagai inisialisasi awal, diberikan matriks $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(Z_n)$ dan vektor $C=\begin{pmatrix} s \\ t \end{pmatrix} \in Z_n^2$, serta suatu permutasi $p=\begin{pmatrix} 1 & 2 & \cdots & 10 \\ p(1) & p(2) & \cdots & p(10) \end{pmatrix} \in S_{10}$. Fungsi affine yang digunakan adalah:

$$AX + C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_q \\ x_r \end{pmatrix} + \begin{pmatrix} s \\ t \end{pmatrix} \pmod n$$

Diberikan kunci $K = k_1k_2\ k_3k_4\ k_5k_6\ k_7k_8\ k_9k_{10}$, dengan $k_i \in Z_n$, $i = 1,2,...,10$. Untuk putaran ke-1 dilakukan pergeseran kunci sebanyak satu, yaitu $K^1 = k_2k_3\ k_4k_5\ k_6k_7\ k_8k_9\ k_{10}k_1$, untuk putaran ke-2, dilakukan pergeseran lagi pada K^1, yaitu $K^2 = k_3k_4\ k_5k_6\ k_7k_8\ k_9k_{10}\ k_1k_2$, demikian seterusnya. Berikut ini diberikan algoritma enkripsi selengkapnya.

Algoritma 1: Algoritma Enkripsi

Input:

- Plainteks $X = x_1x_2\ x_3x_4\ x_5x_6\ x_7x_8\ x_9x_{10}$
- Kunci $K = k_1k_2\ k_3k_4\ k_5k_6\ k_7k_8\ k_9k_{10}$
- Jumlah putaran = *m*

Outuput: Cipherteks $Y = y_1y_2\ y_3y_4\ y_5y_6\ y_7y_8\ y_9y_{10}$

Langkah-langkah:

1. Jumlahkan plainteks *X* dengan kunci awal *K*, yaitu $f_i \leftarrow (x_i + k_i) \bmod n$, sehingga diperoleh $F = f_1f_2\ f_3f_4\ f_5f_6\ f_7f_8\ f_9f_{10}$.
2. Untuk *i* dari 1 sampai dengan *m*, lakukan:

2.1. Potong *F* menjadi blok-blok dengan panjang dua. Ubah ke bentuk vektor, yaitu

$$F_{12} = \begin{pmatrix} f_1 \\ f_2 \end{pmatrix},\ F_{34} = \begin{pmatrix} f_3 \\ f_4 \end{pmatrix},\ F_{34} = \begin{pmatrix} f_3 \\ f_4 \end{pmatrix},\ F_{78} = \begin{pmatrix} f_7 \\ f_8 \end{pmatrix} \text{ dan } F_{910} = \begin{pmatrix} f_9 \\ f_{10} \end{pmatrix}.$$

2.2. Untuk setiap $F_{qr} = \begin{pmatrix} f_q \\ f_r \end{pmatrix}$, kalikan dengan matriks *A*, kemudian dijumlahkan dengan vektor *C*, yaitu: $\begin{pmatrix} g_q \\ g_r \end{pmatrix} = AF_{qr} + C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_q \\ x_r \end{pmatrix} + \begin{pmatrix} s \\ t \end{pmatrix}$. Diperoleh

$$G^i = g_1g_2\ g_3g_4\ g_5g_6\ g_7g_8\ g_9g_{10}.$$

2.3. Lakukan permutasi pada *G* menggunakan permutasi *p*, diperoleh

$$H^i = p(g_1)\,p(g_2)\ p(g_3)\,p(g_4)\,p(g_5)\,p(g_6)\ p(g_7)\,p(g_8)\ p(g_9)\,p(g_{10})$$
$$= h_1h_2\ h_3h_4\ h_5h_6\ h_7h_8\ h_9h_{10}$$

2.4. Jumlahkan H dengan K^i yaitu kunci pada putaran ke-*i*. Diperoleh $z_i \leftarrow (h_i + k_i) \bmod n$, yaitu $Z^i = z_1 z_2 \ z_3 z_4 \ z_5 z_6 \ z_7 z_8 \ z_9 z_{10}$.

3. Jumlahkan hasil akhir Z^m dengan kunci awal K, yaitu $y_i \leftarrow (z_i + k_i) \bmod n$. Diperoleh cipherteks $Y = y_1 y_2 \ y_3 y_4 \ y_5 y_6 \ y_7 y_8 \ y_9 y_{10}$.

Algoritma Dekripsi pada dasarnya sama dengan Algoritma Enkripsi, hanya saja menggunakan invers dari fungsi affine dan invers dari permutasi. Diberikan fungsi affine $AX + C$. Misalkan $\begin{pmatrix} v \\ w \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_q \\ x_r \end{pmatrix} + \begin{pmatrix} s \\ t \end{pmatrix}$, maka $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_q \\ x_r \end{pmatrix} = \begin{pmatrix} v \\ w \end{pmatrix} - \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} v-s \\ w-t \end{pmatrix}$, sehingga diperoleh $\begin{pmatrix} x_q \\ x_r \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} v-s \\ w-t \end{pmatrix}$.

Algoritma 2: Algoritma Dekripsi

Input:

- Cipherteks $Y = y_1 y_2 \ y_3 y_4 \ y_5 y_6 \ y_7 y_8 \ y_9 y_{10}$
- Kunci $K = k_1 k_2 \ k_3 k_4 \ k_5 k_6 \ k_7 k_8 \ k_9 k_{10}$
- Jumlah putaran = m

Outuput: Plainteks $X = x_1 x_2 \ x_3 x_4 \ x_5 x_6 \ x_7 x_8 \ x_9 x_{10}$

Langkah-langkah:

1. Kurangkan cipherteks Y dengan kunci awal K, yaitu $f_i \leftarrow (y_i - k_i) \bmod n$, sehingga diperoleh $H = h_1 h_2 \ h_3 h_4 \ h_5 h_6 \ h_7 h_8 \ h_9 h_{10}$.
2. Untuk *i* dari 1 sampai dengan *m*, lakukan:

2.1. Kurangkan H dengan K^i yaitu kunci pada putaran ke-(m-i+1). Diperoleh $z_i \leftarrow (h_i - k_i) \bmod n$, yaitu $Z^i = z_1 z_2 \ z_3 z_4 \ z_5 z_6 \ z_7 z_8 \ z_9 z_{10}$.

2.2. Potong Z menjadi blok-blok dengan panjang dua. Ubah ke bentuk vektor, yaitu $Z_{1,2} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$, $Z_{3,4} = \begin{pmatrix} z_3 \\ z_4 \end{pmatrix}$, $Z_{3,4} = \begin{pmatrix} z_3 \\ z_4 \end{pmatrix}$, $Z_{7,8} = \begin{pmatrix} z_7 \\ z_8 \end{pmatrix}$ dan $Z_{9,10} = \begin{pmatrix} z_9 \\ z_{10} \end{pmatrix}$.

2.3. Lakukan permutasi pada Z menggunakan invers permutasi dari p, yaitu $p^{-1} = \begin{pmatrix} 1 & 2 & \cdots & 10 \\ p^{-1}(1) & p^{-1}(2) & \cdots & p^{-1}(10) \end{pmatrix} \in S_{10}$, diperoleh

$$F^i = p^{-1}(z_1)\,p^{-1}(z_2)\;p^{-1}(z_3)\,p^{-1}(z_4)\,p^{-1}(z_5)\,p^{-1}(z_6)\;p^{-1}(z_7)\,p^{-1}(z_8)\;p^{-1}(z_9)\,p^{-1}(z_{10})$$
$$= f_1 f_2\;\; f_3 f_4\;\; f_5 f_6\;\; f_7 f_8\;\; f_9 f_{10}$$

$F_{1,2} = \begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$, $F_{3,4} = \begin{pmatrix} f_3 \\ f_4 \end{pmatrix}$, $F_{3,4} = \begin{pmatrix} f_3 \\ f_4 \end{pmatrix}$, $F_{7,8} = \begin{pmatrix} f_7 \\ f_8 \end{pmatrix}$ dan $F_{9,10} = \begin{pmatrix} f_9 \\ f_{10} \end{pmatrix}$.

2.4.Untuk setiap $F_{qr} = \begin{pmatrix} f_q \\ f_r \end{pmatrix}$, kurangkan dengan vektor $C = \begin{pmatrix} s \\ t \end{pmatrix}$, yaitu $\begin{pmatrix} (f_q - s) \bmod n \\ (f_r - t) \bmod n \end{pmatrix}$, kemudian kalikan dengan invers dari matriks A, yaitu $\begin{pmatrix} g_q \\ g_r \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} f_q - s \\ f_r - t \end{pmatrix}$. Diperoleh $G^i = g_1 g_2\;\; g_3 g_4\;\; g_5 g_6\;\; g_7 g_8\;\; g_9 g_{10}$

3. Kurangkan hasil akhir G^m dengan kunci awal K, yaitu $y_i \leftarrow (g_i - k_i) \bmod n$. Diperoleh plainteks $X = x_1 x_2\;\; x_3 x_4\;\; x_5 x_6\;\; x_7 x_8\;\; x_9 x_{10}$.

Sebagai contoh, misalkan Alice ingin mengirimkan pesan rahasia **"matematika"** kepada Bob menggunakan kunci rahasia **"abcdefghij"**. Sebagai inisialisasi awal, keduanya sepakat menggunakan ring komutatif $Z_{26} = \{0,1,2,...,25\}$ yang berkorespondensi dengan himpunan semua huruf alfabet, yaitu $0 \leftrightarrow$ a, $1 \leftrightarrow$ b, $2 \leftrightarrow$ c, dan seterusnya sampai dengan $25 \leftrightarrow$ z. Diperoleh plainteks dan kunci yaitu:

X = 12 0 19 4 12 0 19 8 10 0 dan K = 0 1 2 3 4 5 6 7 8 9

Keduanya sepakat menggunakan matriks $A = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \in GL_2(Z_{26})$, vektor konstan $C = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$ dan permutasi $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 1 & 6 & 10 & 8 & 9 & 3 & 4 & 2 \end{pmatrix} \in S_{10}$. Dapat ditunjukkan bahwa matriks A tersebut mempunyai invers $A^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$ dan permutasi p tersebut mempunyai invers yaitu permutasi

$p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 8 & 9 & 2 & 4 & 1 & 6 & 7 & 5 \end{pmatrix}$. Inisialisasi tersebut bersifat umum, artinya boleh diketahui siapa saja, yang dirahasiakan adalah plainteks dan kunci. Keduanya sepakat menggunakan iterasi sebanyak 3. Diperoleh penjadwalan kunci:

$K^1 = 1\,2\,3\,4\,5\,6\,7\,8\,9\,0$, $K^2 = 2\,3\,4\,5\,6\,7\,8\,9\,0\,1$, $K^3 = 3\,4\,5\,6\,7\,8\,9\,0\,1\,2$

Proses enkripsi diberikan dalam tabel sebagai berikut.

Tabel 2. Proses Enkripsi Jaringan-Substitusi Permutasi atas Z_{26}

	1	2	3	4	5	6	7	8	9	10
X	12	0	19	4	12	0	19	8	10	0
F	12	1	21	7	16	5	25	15	18	9
$\boldsymbol{G^1}$	20	11	11	2	18	25	15	18	15	18
$\boldsymbol{H^1}$	11	18	18	15	11	2	20	25	15	18
$\boldsymbol{Z^1}$	12	20	21	19	16	8	1	7	24	18
$\boldsymbol{G^2}$	16	14	3	8	16	20	25	20	25	20
$\boldsymbol{H^2}$	3	20	20	25	14	8	16	20	25	16
$\boldsymbol{Z^2}$	5	23	24	4	20	15	24	3	25	17
$\boldsymbol{G^3}$	15	14	20	16	12	3	12	9	12	9
$\boldsymbol{H^3}$	20	9	9	12	14	16	15	3	12	12
$\boldsymbol{Z^3}$	23	13	14	18	21	24	24	3	13	14
Y	23	24	26	21	25	3	4	10	21	23

Diperoleh cipherteks Y = 23 24 26 21 25 3 4 10 21 23 yang berkorepondensi dengan "**xoqvzdekvx**". Selanjutnya, cipherteks ini dikirimkan oleh Alice kepada Bob. Apabila ada pihak ketiga yaitu Eve yang berhasil menyadap pesan ini, maka Eve hanya mengetahui cipherteks dan inisialisasi algoritma berupa matriks, vektor, permutasi dan jumlah iterasi. Untuk memecahkan plainteks, Eve harus menemukan kunci yang digunakan oleh Alice. Semakin banyak jumlah iterasi, maka Eve menjadi lebih sulit untuk menemukan kuncinya. Sebagai contoh, pada contoh di atas untuk iterasi sebanyak 100 kali akan menghasilkan cipherteks **"jqsnipyxxr"**. Jika kunci dirubah sedikit menjadi **"bbcdefghij"**, dengan iterasi sebanyak 100 kali akan menghasilkan cipherteks **"cxzsmxuicb"**. Terlihat bahwa perubahan sedikit saja pada kunci akan menghasilkan cipherteks yang sangat berbeda. Untuk proses dekripsi dari contoh di atas dapat

dipelajari dari Algoritma 2 yang telah diberikan menggunakan invers matriks dari *A* dan invers permutasi dari *p*.

4. Kesimpulan dan Saran

Proses enkripsi menggunakan Jaringan Substitusi-Permutasi dapat diterapkan pada suatu ring komutatif Z_n menggunakan substitusi dengan fungsi affine berupa perkalian matriks dan penjumlahan vektor. Akan tetapi, untuk menjamin bahwa proses dekripsi akan berjalan adalah dengan mensyaratkan bahwa matriks yang digunakan dalam proses substitusi harus invertibel atas Z_n, artinya determinan dari matriks tersebut relatif prima dengan *n*. Untuk meningkatkan keamanan, sebaiknya iterasi dilakukan dalam jumlah yang banyak, seperti lebih dari 1000 kali. Hal ini dilakukan agar cipherteks terlihat benar-benar acak, walaupun kunci dirubah sedikit. Selanjutnya, perlu dikaji lebih lanjut mengenai keamanan dari algoritma tersebut menggunakan analisis secara statisitik dan teori probabilitas. Hal ini perlu dilakukan untuk mengetahui tingkat keacakan dan keterkaitan antara plainteks, kunci dan cipherteks.

Daftar Pustaka

Menezes Alfred J., Paul C. van Oorschot dan Scott A. Vanstone, 1996, *Handbook of Applied Cryptography*, CRC Press, USA.

Stinson, Douglas R., 2006, *Cryptography Theory and Practice, Third Edition*, Chapman & Hall/CRC, Florida.